JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Jacqueline Minka, Bryan Minka, Shayna Spivak, Charles Derr, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff: Montgomery County, PA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Charles J. Kocher, Patrick Howard - Saltz, Mongeluzzi, Barrett & Bendesky, PC - 120 Gibraltar Rd., Ste. 218, Horsham, PA 19044
(215) 575-3985

DEFENDANTS

Equifax Information Services, Inc.

County of Residence of First Listed Defendant: Fulton County, GA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☒ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
Fair Credit Reporting Act, 15 U.S.C. §§ 1681 - 1681x

Brief description of cause:
Violation of statute regarding data breach of personal identifying information of Plaintiffs

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE ______ DOCKET NUMBER ______

DATE: 9-20-2017

SIGNATURE OF ATTORNEY OF RECORD: [signature]

FOR OFFICE USE ONLY

RECEIPT # ______ AMOUNT ______ APPLYING IFP ______ JUDGE ______ MAG. JUDGE ______

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JACQUELINE MINKA, BRYAN MINKA, SHAYNA SPIVAK, CHARLES DERR, *Individually, and on behalf of all others similarly situated,*	:	CIVIL NO. ____________
Plaintiffs,	:	COMPLAINT – CLASS ACTION
v.	:	JURY TRIAL DEMANDED
EQUIFAX INFORMATION SERVICES, INC.,	:	
Defendant.	:	

CLASS ACTION COMPLAINT

I. INTRODUCTION

1. This is a Complaint brought by Plaintiffs and those similarly situated, against Defendant Equifax Information Services, Inc. ("Defendant" or "Equifax"). Plaintiffs' allegations with respect to themselves are based on personal knowledge and, as to all other matters, on information and belief derived from a review of public documents and the investigation of Plaintiffs' counsel.

2. On September 7, 2017, Equifax announced a nationwide data breach affecting an estimated 143 million consumers (the "Data Breach"). Equifax's disclosure, which came more than five weeks after the Company claims to have learned of the breach, states that unauthorized parties accessed consumers' sensitive, personal information maintained by Equifax by exploiting a website application vulnerability. Equifax claims that, based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information included names, addresses, Social Security numbers, dates of birth, and, in some instances, driver's license numbers. Equifax also admitted that credit card numbers for approximately 209,000

consumers, and certain dispute documents with personal identifying information ("PII") for approximately 182,000 consumers were accessed.

3. Equifax is a global giant in the business of maintaining and using private, sensitive consumer information. While primarily known as a consumer reporting agency, Equifax has expanded its information collection and dissemination services to include subscription-based credit monitoring and identity theft protection services for consumers and payroll and human resources services. According to Equifax it "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide[.]"

4. As part of its business, Equifax collects and organizes personal private information about consumers, including Plaintiffs and other class members. Equifax obtains consumers' PII from the services it provides, as well as from credit card companies, banks, credit unions, retailers, auto and mortgage lenders, and other sources that provide PII to Equifax and other credit reporting agencies. Equifax disseminates this PII, which includes consumer credit scores, credit histories, and risk analysis to lenders, retailers, automotive dealers, and mortgage companies. This PII determines an individual's creditworthiness, which can affect their ability to gain loans, housing and jobs.

5. Equifax also is in the business of selling credit and identity theft protection services to consumers – a highly lucrative business in which it makes many millions of dollars.

6. Plaintiffs and the other class members reasonably expect and believe that Equifax will take appropriate measures to protect their PII. Equifax informs customers that it will protect their PII. According to Equifax, it has "built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy

and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."

7. The Data Breach occurred because Equifax failed to implement adequate security measures to safeguard Plaintiffs' and other consumers' PII and willfully ignored known weaknesses in its data security, including prior hacks into its information systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a large number of individuals' valuable PII.

8. As the result of Equifax's inadequate cybersecurity, armed with the personal information obtained in the Data Breach, identity thieves can commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, and open financial accounts and credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other criminals who intend to misuse the information.

9. Astonishingly, Equifax admittedly knew of the authorized access as early as July 29, 2017 but failed to make any public disclosure until September 7, 2017 – over a month after the Data Breach.

10. And to add insult to injury, at least three Equifax executives – including Equifax's CFO – protected themselves by dumping substantial holdings of Equifax stock days after learning of the breach – but still over a month before Equifax informed Plaintiffs and the public

at large. At the time of filing, these stock sales are the focus of a federal criminal probe. https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe (last visited on September 18, 2017).

11. This class action seeks to remedy all of these inexcusable failings. Plaintiffs bring this action on behalf of themselves and on behalf of persons whose PII was disclosed as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

12. As a result of the Data Breach, the PII of Plaintiffs and the class members have been exposed to criminals for misuse. The injuries suffered, or likely to be suffered, by Plaintiffs and the class members include:

a. unauthorized use of their PII;

b. theft of personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and class members' information on the Internet black market;

h. the loss of Plaintiffs' and class members' privacy.

13. The injuries to Plaintiffs and class members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII.

14. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Equifax is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII was stolen as a result of the Equifax Data Breach.

15. Importantly, Plaintiffs and the class members cannot just stop using Equifax, unless they want to stop using credit. "The information in your credit report goes directly to Equifax from any company that has, does or would like to extend you credit. That includes your credit card companies, banks, credit unions, retailers, auto loan and mortgage lender."[1]

16. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

---

[1] http://money.cnn.com/2017/09/11/pf/equifaxmyths/index.html (last visited on September 14, 2017).

II. PARTIES

PLAINTIFFS

17. Plaintiff Jacqueline Minka is a citizen of Pennsylvania and resides in East Norriton, Pennsylvania. She is a victim of the Data Breach. Plaintiff Jacqueline Minka has spent time and effort monitoring her financial accounts.

18. Plaintiff Bryan Minka is a citizen of Pennsylvania and resides in East Norriton, Pennsylvania. He is a victim of the Data Breach. Plaintiff Bryan Minka has spent time and effort monitoring his financial accounts.

19. Plaintiff Shayna Spivak is a citizen of New Jersey and resides in Marlton, New Jersey. She is a victim of the Data Breach. Plaintiff Spivak has spent time and effort monitoring her financial accounts.

20. Plaintiff Charles Derr is a citizen of New Jersey and resides in Marlton, New Jersey. He is a victim of the Data Breach. Plaintiff Derr has spent time and effort monitoring his financial accounts.

DEFENDANT

21. Defendant Equifax, upon information and belief, is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE, Atlanta, Georgia 30309. Equifax regularly conducts business in this District.

22. Equifax is one of the major credit reporting bureaus in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services for individuals, businesses, and compliance with government regulations. Specifically, Equifax provides business services to the automotive, communications, utilities and digital media, education, financial services, healthcare, insurance, mortgage, restaurant, retail and wholesale trade,

staffing, and transportation and distribution industries.[2] Equifax markets and sells many products to consumers and businesses, including Consumer Reports, which provides "access to current personally identifiable information for over 210 million consumers."[3] According to Equifax, "[o]ur consumer data is updated daily from multiple sources to give you the most recent and freshest decisioning perspective available."[4] Equifax's Consumer Reports also includes "tradelines on over 1.8 billion trades updated monthly" and "600 million unique, annual inquiries." Equifax's Consumer Reports provides "access to the consumer's name, current address, address, previous former addresses, birth date, former names and Social Security number." Equifax's Consumer Reports is a product designed to "increase revenue":[5]

> **Make effective decisions that increase revenue**
>
> Trust Equifax Consumer Reports to deliver the powerful combination of predictive consumer credit data and proven expertise backed by unmatched industry leadership. Make faster decisions with the competitive advantage of data speed and system integrity. Strengthen predictive ability, mitigate risk, manage acquisition costs and increase revenue with proven decisioning insight from Equifax Consumer Reports.

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1337, as well as jurisdiction over the state law claims pursuant to 28 U.S.C. §§ 1332(d)(2) and 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs. There are more than 100 putative class members. And almost all members of the proposed class have a different citizenship from Equifax.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because the Defendant regularly transacts business within this district and because a substantial part of the events giving

---

[2] *See Equifax's Business Industries*, EQUIFAX, http://www.equifax.com/business/ (last visited Sept. 14, 2017).
[3] *See Equifax's Consumer Reports Product Overview*, EQUIFAX, http://www.equifax.com/business/consumer-reports (last visited Sept. 14, 2017).
[4] *Id.*
[5] *See Equifax's Consumer Reports Product Sheet*, EQUIFAX, http://www.equifax.com/assets/USCIS/efx-00198_consumer_reports.pdf (last visited Sept. 14, 2017).

rise to the claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach Compromised the PII of 143 Million Consumers

25. Equifax generates billions of dollars in revenue each year collecting, using, and reporting on consumer PII.

26. Plaintiffs and the class members had entrusted Equifax to safeguard their PII. Equifax owes Plaintiffs and the class members a duty to use reasonable care to protect their PII from unauthorized access. Equifax has publically acknowledged, through its Privacy Policy, that it purportedly takes steps "to protect the privacy and confidentiality of personal information about consumers" and that "[s]afeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."[6]

27. On September 7, 2017, Equifax announced that its systems had been breached and that the Data Breach affected approximately 143 million consumers. According to Equifax's website regarding the Data Breach, unauthorized users acquired the PII of approximately 143 million consumers from certain files maintained and stored by Equifax. The PII included names, addresses, Social Security numbers, dates of birth, and, in some instances, driver's license numbers, and other personal information:

> **Equifax Announces Cybersecurity Incident Involving Consumer Information**
>
> September 7, 2017— Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no

[6] http://www.equifax.com/cs/Satellite/EFX_Content_C1/1169228061187/5-1/5-1_Layout.htm?packedargs=Locale%3Den_US (last visited on September 14, 2017).

evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one

> year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.
>
> In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries. Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.
>
> CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."[7]

28. The Equifax announcement came more than five weeks after the Company first learned of the data breach. Equifax has provided no explanation as to why it waited weeks before warning people impacted by the breach that their critical PII had been accessed and stolen by unknown hackers. Remarkably, even while Equifax was failing to notify people impacted by the breach, thereby preventing the millions of impacted people from taking steps to protect themselves, several high level executives at the Company, including Chief Financial Officer John Gamble, engaged in sales of Equifax stock, selling approximately $1.8 million in stock in the days after the Company learned of the Data Breach – and before the Company's stock would inevitably fall once the massive Data Breach was announced.

29. On its Data Breach website, Equifax invites individuals to determine if their

[7] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 (last visited September 14, 2017).

personal information may have been impacted by the Data Breach by providing their last name and the last six digits of their Social Security number. If an individual is determined to have been affected, Equifax provides them with a date to return to the website to enroll in Equifax's TrustedID Premier credit monitoring service. If an individual is determined to have not been affected, Equifax provides them with this information, but then still provides them with a link to enroll in Equifax's TrustedID Premier credit monitoring service. This product falls short of correcting the massive, irreparable harm caused by the Data Breach.

30. Equifax had initially requested that consumers waive various legal rights to access the TrustedID Premier credit monitoring service. However, on or about September 11, 2017, Equifax reversed its position by removing these illegal and unenforceable terms from its website. *See* https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited on September 12, 2017) ("To confirm, enrolling in the free credit file monitoring and identity theft protection products that we are offering as part of this cybersecurity incident does not prohibit consumers from taking legal action. We have already removed that language from the Terms of Use on the site www.equifaxsecurity2017.com. The Terms of Use on www.equifax.com do not apply to the TrustedID Premier product being offered to consumers as a result of the cybersecurity incident. Again, to be as clear as possible, we will not apply any arbitration clause or class action waiver against consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.").

B. Equifax Failed to Timely Disclose the Data Breach

31. According to Equifax, the hackers had access to the aforementioned sensitive, personal information of 143 million Americans from at least May 2017 until July 29, 2017, when the intrusion was discovered.

32. Equifax's preliminary investigation found the breach was due to its error – a

vulnerability in an application in its U.S. website – which allowed hackers access to certain files.

33. While Equifax learned of the Data Breach on or before July 29, 2017, it waited for more than a month before informing the public. As of filing this complaint, Plaintiffs and Class members affected by the Data Breach still have not been personally notified by Equifax.

34. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions", including credit reporting agencies such as Equifax, "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. §6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. §6801(b) (emphasis added).

35. In order to satisfy their obligations under the GLBA, financial institutions must "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. §314.3.

36. Under the Interagency Guidelines Establishing Information Security Standards, 12 CFR Appendix D-2 to Part 208, financial institutions have an affirmative duty to "develop

and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* at Supplement A, §II.

37. Further, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *See id.* at Supplement A, §III.A.

38. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

39. Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to: (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Plaintiffs' and class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Plaintiffs' and class members' PII.

40. Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[.]" This includes, but is not limited to, Equifax's failure to notify the affected

individuals themselves of the Data Breach in a timely and adequate manner.

C. Equifax Failed to Honor Its Promises to Keep Sensitive Personal Information Confidential

41. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting consumers who have encountered a data breach. This includes credit-monitoring and identity-theft protection products to guard consumers' personal information.

42. Equifax describes itself as a "global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions."[8]

43. Equifax says that it "develop[s], maintain[s] and enhance[s] secured proprietary information databases through the compilation of consumer specific data, including credit, income, employment, asset, liquidity, net worth and spending activity, and business data, including credit and business demographics, that we obtain from a variety of sources, such as credit granting institutions, income and tax information primarily from large to mid-sized companies in the U.S., and survey-based marketing information. We process this information utilizing our proprietary information management systems. We also provide information, technology and services to support debt collections and recovery management."[9]

44. Equifax concedes that "[b]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debt management and human resources-related services. We also offer a portfolio of

---

[8] *See* http://www.equifax.com/about-equifax/company-profile/ (last visited September 14, 2017).
[9] *See* https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm *at 60* (last visited September 14, 2017).

products that enable individual consumers to manage their financial affairs and protect their identity."[10]

45. Although Equifax knows about the vulnerabilities of its online website applications and databases and lack of internal supervisory mechanisms, Equifax continued to represent and promise that consumers' personal and private information was safe and secure.

46. Equifax is well aware of the dangers of identity theft cautioning consumers that "[i]dentity theft is committed when someone steals your personal information – such as your name, Social Security number, and date of birth – typically to hijack your credit and use it to open up new credit accounts, take out loans in your name, or access your bank or retirement accounts. An identity thief can even use your personal information to steal your tax refunds, seek medical services, or commit crimes in your name."[11]

47. Equifax acknowledges that "[o]nce an identity thief has access to your personal information, he or she can also:

- Open new credit card accounts with your name, Social Security number and date of birth. When the thief charges to the credit cards and leaves the bills unpaid, the delinquency will be reported to your credit report and could impact your credit score;
- Open a bank account in your name and write bad checks on the account;
- Create counterfeit checks or debit cards and use them to drain your existing bank accounts;
- File for bankruptcy under your name to avoid paying debts;
- Set up a phone, wireless, or other utility service in your name."[12]

---

[10] *Id.* at 29.
[11] *See* https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft (last visited September 14, 2017).
[12] *Id.*

48. At all relevant times, Equifax designed and implemented its policies and procedures regarding the security of protected financial information and sensitive information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected financial information and other sensitive information.

49. Plaintiffs and Class members relied on Equifax to keep their sensitive information safeguarded and otherwise confidential.

50. Equifax unreasonably and negligently failed to take appropriate steps to store and secure Plaintiffs' and the class members' PII.

51. As a direct and proximate result of Equifax's actions and omissions, Plaintiffs and similarly situated consumers have been harmed, injured, and damaged. Plaintiffs and class members have been injured through unauthorized use of their PII and through violations of statutes such as the FCRA and the GLBA that recognize the inherent harm in such unauthorized access to and use of PII, as well as the multitude of harms that are likely to follow from such access and use. Consumers like Plaintiffs already have had to spend time and resources trying to redress the effects of the breach, including investigating the extent to which their PII has been compromised and putting in place credit monitoring and credit freezes to try to minimize the risks to which they have been exposed. These harms were reasonably foreseeable to Equifax.

V. CLASS ACTION ALLEGATIONS

52. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide Class defined as follows:

> All United States residents whose personally identifiable information ("PII") was accessed without authorization in the data breach announced by Equifax in September 2017 (the "Nationwide Class").

53. Pursuant to Fed. R. Civ. P. 23, and in the alternative and/or in addition to claims

asserted on behalf of a Nationwide Class, Plaintiffs Jacqueline and Bryan Minka assert claims under the FCRA and the laws of the Commonwealth of Pennsylvania, and on behalf of a separate Pennsylvania Class, defined as follows:

> All persons residing in Pennsylvania whose personally identifiable information was acquired without authorization in the data breach announced by Equifax in September 2017 (the "Pennsylvania Class").

54. Pursuant to Fed. R. Civ. P. 23, and in the alternative and/or in addition to claims asserted on behalf of a Nationwide Class, Plaintiffs Derr and Spivak assert claims under the FCRA and the laws of New Jersey, and on behalf of a separate New Jersey Class, defined as follows:

> All persons residing in New Jersey whose personally identifiable information was acquired without authorization in the data breach announced by Equifax in September 2017 (the "New Jersey Class").

55. Excluded from each of the above classes are Equifax and any of its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the class; government entities; all counsel for Plaintiffs and Equifax; and the judges to whom this case is assigned and their immediate family and court staff.

56. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

57. Each of the proposed classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

Numerosity

58. While the exact number of Class members is unknown, Equifax has admitted the personal information, including names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers of approximately 143 million Americans was taken during the Data Breach. Plaintiffs therefore believe that the Class is so numerous that joinder of

all members is impractical. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

Commonality

59. There are numerous questions of law and fact common to Plaintiffs and the Classes, including the following:

a. Whether Equifax has engaged in unlawful, unfair or fraudulent business acts or practices;

b. Whether Equifax has engaged in the wrongful conduct alleged herein;

c. Whether Equifax had a duty to protect PII;

d. Whether Equifax used reasonable or industry standard measures to protect Class members' personal and financial information, particularly in light of the measures recommended by data security experts;

e. Whether Equifax adequately or properly segregated its network so as to protect personal customer data;

f. Whether Equifax knew or should have known prior to the security breach that its network was susceptible to a potential data breach;

g. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

h. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

i. Whether Equifax should have notified the Class that it failed to use reasonable and best practices, safeguards, and data security measures to protect customers' personal and financial information;

j. Whether Equifax should have notified Class members that their personal and financial information would be at risk of unauthorized disclosure;

k. Whether Equifax intentionally failed to disclose material information regarding its security measures, the risk of data interception, and the Data

Breach;

l. Whether Equifax's acts, omissions, and nondisclosures were intended to deceive Class members;

m. Whether Equifax's conduct violated the laws alleged;

n. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class members;

o. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and,

p. Whether Plaintiffs and the Class members are entitled to restitution, disgorgement, and other equitable relief;

q. Whether Plaintiffs and the Class members are entitled to recover actual damages, statutory damages, and punitive damages.

Typicality

60. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs each had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other class members and Plaintiffs seek relief consistent with the relief of the Classes. Plaintiffs and the Class members were injured by the same wrongful acts, practices, and omissions committed by Equifax, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

Fair and Adequate Representation

61. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests which are adverse to or conflict with those of the Class members Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

The Prerequisites of Rule 23(b)(3) are Satisfied

62. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

63. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. The damages suffered by Plaintiffs and the Class members are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Injunctive and Declaratory Relief

64. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

65. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are

not limited to:

a. Whether Equifax failed to timely notify the public of the Data Breach;

b. Whether Equifax owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Equifax failed to take commercially reasonable steps to safeguard the PII of Plaintiffs and the Class members; and,

f. Whether adherence to data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

66. Finally, all members of the proposed classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the Class members can be identified and their contact information ascertained for purposes of providing notice to the Class members.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

[ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS JACQUELINE AND BRYAN MINKA AND THE PENNSYLVANIA CLASS AND PLAINTIFFS SPIVAK AND DERR AND THE NEW JERSEY CLASS]

67. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

68. Upon accepting and storing the PII of Plaintiffs and the Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

69. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

70. Equifax owed numerous duties to Plaintiffs and to the Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

71. Equifax also breached its duty to Plaintiffs and the Class members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without

consent.

72. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

73. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' PII.

74. Equifax breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members.

75. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

76. Equifax had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

77. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

78. Equifax also had independent duties under state and federal laws that required

Equifax to reasonably safeguard Plaintiffs' and Class members' PII and promptly notify them about the data breach.

79. Equifax breached its duties to Plaintiffs and the Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs' and Class members' PII had been improperly acquired or accessed.

80. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax possession or control.

81. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse

consequences, and thwart future misuse of their PII.

82. Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class members and then by failing to provide Plaintiffs and Class members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class members.

83. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax's possession or control.

84. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

85. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiffs and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

86. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

87. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

88. As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees charges and foregone cash back rewards; and/or damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events

surrounding the theft mentioned above.

COUNT II

NEGLIGENCE PER SE

[ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS JACQUELINE AND BRYAN MINKA AND THE PENNSYLVANIA CLASS AND PLAINTIFFS SPIVAK AND DERR AND THE NEW JERSEY CLASS]

89. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

90. Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1). The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

91. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class members.

92. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

93. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

94. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the

Class.

95. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Class members have suffered, and continue to suffer, injuries damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees, charges and foregone cash back rewards; and/or damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

96. Equifax also violated the GLBA (Graham-Leach-Biley Act), 15 U.S.C. § 6801(b), because, among other things, Equifax failed to maintain and follow a written information security protocol with "administrative, technical, and physical safeguards" commensurate with the "size and complexity" of its business, the "nature and scope" of its activities, and, importantly, "the sensitivity of [the] consumer information at issue." 16 C.F.R. § 314.4.

97. Equifax's violations of the GLBA constitute negligence per se.

98. Plaintiffs and the Class members were foreseeable victims of Equifax's violations of its statutory and regulatory duties. The GLBA, for example, was enacted "to insure the security and confidentiality of customer records and information," "to protect against any anticipated threats or hazards to the security or integrity of such records," and "to protect against

unauthorized access to or use of such records or information which could results in substantial harm or inconvenience to any customer." 15 U.S.C. § 6801(b).

99. Equifax's breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiffs and the Classes without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized access.

100. Equifax's breach of its duties has direct and proximately injured Plaintiffs and the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (nor or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

101. Plaintiffs and the Classes are entitled to damages in an amount to be proven at trial.

COUNT III

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

[ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE PENNSYLVANIA CLASS]

102. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

103. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

104. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties ...." 15

U.S.C. § 1681a(f).

105. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

106. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to ... limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

107. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit ... to be used primarily for personal, family, or household purposes; ... or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

108. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting

agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

109. Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

110. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

111. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

112. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other Class members of their rights under the FCRA.

113. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

114. Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer ... or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

115. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT IV

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

[ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS JACQUELINE AND BRYAN MINKA

AND THE PENNSYLVANIA CLASS AND PLAINTIFFS SPIVAK AND DERR AND THE NEW JERSEY CLASS]

116. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

117. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

118. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

119. Plaintiffs and the Nationwide Class members have been damaged by Equifax's negligent failure to comply with the FCRA, including by paying out of pocket costs to institute credit freezes with the nations consumer reporting agencies so that their credit cannot be accessed and misused as a result of the Data Breach. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

120. Plaintiffs and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT V

DECLARATORY JUDGMENT

[ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS JACQUELINE AND BRYAN MINKA AND THE PENNSYLVANIA CLASS AND PLAINTIFF SPIVAK AND PLAINTIFF DERR AND THE NEW JERSEY CLASS]

121. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

122. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

123. Equifax still possesses PII pertaining to Plaintiffs and Class members.

124. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

125. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

126. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

127. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

COUNT VI

VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. § 201-1, *et seq.*

[ON BEHALF OF PLAINTIFFS JACQUELINE AND BRYAN MINKA AND THE PENNSYLVANIA CLASS]

128. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

129. Plaintiffs Jacqueline and Bryan Minka and members of the Pennsylvania Class are "persons" within the meaning of 73 P.S. § 201-2(2).

130. Equifax is engaged in "trade" or "commerce" within the meaning of 73 P.S. § 201-2(3).

131. The Pennsylvania Unfair Trade Practices Act ("Pennsylvania UTPCPL") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce ...." 73 P.S. § 201-3.

132. As alleged throughout this Complaint, Equifax's deliberate conduct constitutes deceptive acts or practices in the conduct of business trade or commerce and furnishing of services including:

a. Failure to maintain adequate computer systems and data security practices to safeguard consumers' PII;

b. Failure to disclose that its computer systems and data security practices were inadequate to safeguard consumers' PII from theft; and

c. Failure to timely and accurately disclose the data breach to consumer Plaintiffs and Pennsylvania Class members.

d. Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. Continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

133. Plaintiffs Jacqueline and Bryan Minka and the Pennsylvania Class members relied upon Equifax's deceptive and unlawful conduct.

134. Plaintiff Jacqueline and Bryan Minka and Pennsylvania Class members

entrusted Equifax with their PII.

135. Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and violates the Pennsylvania UTPCPL.

136. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs Jacqueline and Bryan Minka and Pennsylvania Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

137. As a direct and proximate result of Equifax's violation of the Pennsylvania UTPCPL, Plaintiffs Jacqueline and Bryan Minka and Pennsylvania Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Pennsylvania Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including, but not limited to, late fees, charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation

of the facts and events surrounding the theft mentioned above.

138. Equifax's actions and conduct in violating 73 P.S. § 201-1, *et seq*. have caused, or are likely to cause, substantial damage to Plaintiffs Jacqueline and Bryan Minka and Pennsylvania Class Members that includes:

a. Fraudulent charges on their debit and credit card accounts which may not be reimbursed;

b. Theft of their PII by criminals;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the fraudulent use of their financial accounts;

e. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and list time associated with handling the administrative consequences of the Equifax data breach, including identifying, disputing and seeking reimbursement for fraudulent changes, cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection; and

g. Impairment to their credit scores and ability to borrow and/or obtain credit; and the continued risk to their PII which remains on Equifax's insufficiently secured systems.

139. As a result of Equifax's deceptive conduct, Plaintiffs Jacqueline and Bryan Minka and the Pennsylvania Class are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Equifax because of its deceptive acts and practices, attorney's fees and costs, declaratory relief and a permanent injunction enjoining Equifax from its deceptive trade practices.

140. Also as a direct result of Equifax's knowing violation of 73 P.S. § 201-1, *et seq.*, Plaintiffs Jacqueline and Bryan Minka and Pennsylvania Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

141. Plaintiffs Jacqueline and Bryan Minka bring this action on behalf of herself and Pennsylvania Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs Jacqueline and Bryan Minka and Pennsylvania Class and members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

142. Accordingly, Plaintiffs Jacqueline and Bryan Minka and the Pennsylvania Class also seek damages, equitable relief, and reasonable attorney's fees and costs.

COUNT VII

VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT

[ON BEHALF OF PLAINTIFF SPIVAK AND PLAINTIFF DERR AND THE NEW JERSEY CLASS]

143. Plaintiffs restate and reallege the paragraphs above as if fully set forth herein.

144. Equifax, while operating in New Jersey, engaged, in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes:

a. Collecting, storing, and using vast quantities of highly sensitive PII concerning consumers in on-line, aggregated form over which the consumers themselves exercise no control and which Equifax failed to adequately protect from unauthorized and/or criminal access in violation of statutory and industry standards and its assurances to the public and to the entities that provide the PII to Equifax;

b. Failing to employ technology and systems to promptly detect unauthorized access to the PII with which it was entrusted;

c. Unreasonably delaying giving notice to consumers after it became aware of unauthorized access to the PII;

d. Knowingly and fraudulently failing to provide accurate, timely information to consumers about the extent to which their PII has been compromised;

e. Knowingly and fraudulently placing unreasonable and unlawful terms and conditions on consumers obtaining information about the extent to which their PII has been compromised;

f. Knowingly and fraudulently misleading consumers to waive their legal rights in order to obtain information about the extent to which their PII has been compromised; and

g. Knowingly and fraudulently coercing consumers into enrolling in an Equifax product to redress their injuries.

145. Equifax's breach of its duties has directly and proximately caused Plaintiffs Spivak and Derr and the New Jersey Class to suffer an ascertainable loss of money and property, including the loss of their PII, and foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

146. The above unlawful and deceptive acts and practices and acts by Equifax were

immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs Spivak and Derr and the New Jersey Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

147. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs Spivak and Derr and the New Jersey Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

148. Plaintiffs Spivak and Derr and the New Jersey Class seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at trial), treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, requests a judgment against Defendant, as follows:

A. For an order certifying the Classes, pursuant to Rule 23, appointing Plaintiffs as representatives of the Classes, and designating the undersigned as Class Counsel;

B. An Order enjoining Equifax from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Classes' PII;

C. An Order compelling Equifax to employ and maintain appropriate systems and policies to protect consumer PII and to promptly detect, and timely and accurately report, any unauthorized access to that data;

D. For compensatory damages sustained by Plaintiffs and Class members;

E. For equitable, declaratory, and injunctive relief;

F. For payment of costs of suit herein incurred;

G. For both pre-judgment and post-judgment interest on any amounts awarded;

H. For punitive damages;

I. For payment of reasonable attorneys' fees, expert fees, and expenses, as may be allowable under applicable law; and

J. For such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of the Classes, demand a trial by jury as to all issues so triable.

DATE: 9-20-2017

BY: [signature]

Simon B. Paris
Patrick Howard (PA ID #88572)
Charles J. Kocher (PA ID #93141)
SALTZ, MONGELUZZI, BARRETT & BENDESKY, P.C.
120 Gibraltar Road, Suite 218
Horsham, PA 19044
Telephone: (215) 496-8282
Fax: (215) 754-4443
E-mail: sparis@smbb.com
E-mail: phoward@smbb.com
E-mail: ckocher@smbb.com

Attorneys for Plaintiffs and Proposed Classes